Search Engine Discovery

Search engines can be very useful for finding information about the target. Search engines can be used for two things:

- Finding sensitive information on the domain that you are attacking
- Finding sensitive information about the company and its employees in on other parts of the internet. Like forums, newsgroups etc.

Remember that the world is bigger than google. So test out the other search engines.

Baidu, binsearch.info, Bing, DuckDuckGo, ixquick/Startpage, Shodan,PunkSpider

Google is a good tool to learn more about a website.

Finding specific filetypes

```
filetype:pdf
```

Search within webaddress

```
site:example.com myword
```

Find in url

```
inurl:test.com
```

Wild cards

You can use the asterisk to as a wildcard:

```
*
```

Example:

```
"I've been * for a heart"
```

This will return answers where * is anything.

Exclude words

```
-
```

the dash excludes a specific word

This query searches for pages that used the word bananasplit.

```
-banana bananasplit
```

Cached version

So if a website has been taken down you can still find the cached version, of the last time google visited the site

```
cache:website.com
```

https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf

Examples

```
site:com inurl:admin.php
```

More

Here are some more

Great guide for google dorks
https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf

http://www.googleguide.com/advanced_operators_reference.html

http://www.searchcommands.com/

https://support.google.com/websearch/answer/2466433?hl=en

https://www.exploit-db.com/google-hacking-database/